Processing of medical data in the light of new technological and legal challenges

(Przetwarzanie danych medycznych w świetle nowych wyzwań technologicznych i prawnych)

Artur Romaszewski [1, A,D], Wojciech Trąbka [2,A,D], Szczepan Jakubowski [1,B], Mariusz Kielar [1,B], Mariusz Duplaga [1,F], Zbigniew Kopański [1,C,E], Małgorzata Machota [3,B]

Abstract – Introduction. The modern health care system is functioning in the era of dynamic development of technology of processing increasing resources of knowledge and information. It is carried out both in diagnostics and in processes directly related to the performance of medical procedures thanks to improvements in health data processing techniques. At the same time, a large-scale support of both knowledge resources and organizational processes is provided by specially adapted computer systems. Systems belonging to the so-called artificial intelligence are emerging. All these phenomena are related to the generation of more and more data and information about the patient's health.
The aim of the study. The aim of the study was to discuss the most important problems concerning the safety of medical data in the light of new technological and legal challenges.
Selection of material. The search was conducted in the Scopus database using the following terms: medical data security, IT technologies 2016-2019. The literature found in the Google Scholar database was analyzed in terms of the largest number of citations. Such selected literature was used as a material for the preparation of the present paper.
Conclusions. New regulations on the identification of trust services, personal data security and cyber-security will also have a broad application in health care. Most of them were issued in the form of regulations ensuring their universal applicability throughout the EU. Unfortunately, the implementation of new legal solutions at the level of health care may be difficult, if only because of the costs of implementation. Both the highly desirable system of identification of persons providing health services and patients, the universal implementation of trust services and the classification of some hospitals as operators of key services are very high financial burdens for medical entities. On this occasion, we may wonder whether at least some of the required solutions should not be financed by the state, e.g. issuing certificates for advanced electronic signatures and seals or making cloud solutions widely available for keeping electronic medical records.

Key words **-** medical data processing, information technologies, legal regulations in health care.

Streszczenie – Wstęp. Współczesny system ochrony zdrowia funkcjonuje w erze dynamicznego rozwoju technologii przetwarzania zwiększających się zasobów wiedzy oraz informacji. Dokonuje się on zarówno w diagnostyce, jak również w procesach związanych bezpośrednio z wykonywaniem zabiegów medycznych dzięki udoskonaleniom technik przetwarzania danych o stanie zdrowia. Równolegle następuje stosowane na szeroką skalę wspomaganie zasobów zarówno wiedzy, jak i procesów organizacyjnych przez specjalnie przystosowane do tego systemy komputerowe. Pojawiają się systemy zaliczane do tzw. sztucznej inteligencji. Wszystkie powyższe zjawiska związane są z generowaniem coraz większej ilości danych i informacji o stanie zdrowia pacjenta.
Cel pracy. Celem pracy było omówione najważniejsze problemy dotyczące bezpieczeństwa danych medycznych w świetle nowych wyzwań technologicznych i prawnych.
Dobór materiału. Poszukiwania przeprowadzono w bazie Scopus używając pojęć ***:*** bezpieczeństwa danych medycznych, technologie informatyczne 2016-2019r. Znalezione piśmiennictwo w bazie Google Scholar przeanalizowano pod kątem największej liczby cytowań. Tak wyselekcjonowane piśmiennictwo posłużyło za materiał do opracowania niniejszej pracy.
Wnioski. Nowe przepisy dotyczące identyfikacji usług zaufania, bezpieczeństwa danych osobowych i bezpieczeństwa cybernetycznego będą miały również szerokie zastosowanie w opiece zdrowotnej. Większość z nich została wydana w formie rozporządzeń zapewniających ich powszechne stosowanie w całej UE. Niestety, wdrożenie nowych rozwiązań prawnych na poziomie opieki zdrowotnej może być trudne, choćby ze względu na koszty wdrożenia. Zarówno wysoce pożądany system identyfikacji osób świadczących usługi zdrowotne, jak i pacjentów, powszechne wdrażanie usług zaufania oraz klasyfikacja niektórych szpitali jako operatorów kluczowych usług stanowią bardzo duże obciążenie finansowe dla podmiotów medycznych. Przy tej okazji można się zastanowić, czy przynajmniej część wymaganych rozwiązań nie powinna być finansowana przez państwo, np. wydawanie certyfikatów dla zaawansowanych podpisów i pieczęci elektronicznych lub udostępnianie rozwiązań chmury do przechowywania elektronicznej dokumentacji medycznej.

Słowa kluczowe – przetwarzanie danych medycznych, technologie informatyczne, regulacje prawne w ochronie zdrowia.

Author Affiliations:

1. Faculty of Health Sciences, Jagiellonian University, Poland
2. Department of Bioinformatics and Public Health, Faculty of Medicine and Health Sciences, Andrzej Frycz Modrzewski Krakow University, Poland
3. Collegium Masoviense – College of Health Sciences, Poland

Authors' contributions to the article:

A. The idea and the planning of the study
B. Gathering and listing data
C. The data analysis and interpretation
D. Writing the article
E. Critical review of the article
F. Final approval of the article

Correspondence to:

Artur Romaszewski, Medical, Institute of Public Health, Faculty of Health Sciences, Jagiellonian University, Grzegórzecka 20Str.,PL-31-531 Kraków, Poland, e-mail: artur. romaszewski @uj.edu.pl

Accepted for publication: August 30, 2019.

I. INTRODUCTION

Recent years in the healthcare sector have undoubtedly been a time of information technology development. This development concerns both technical devices used in diagnostics and processes directly related to the performance of medical procedures, as well as new and improved techniques of processing health data. There is also a large-scale support of knowledge resources and organizational processes by specially adapted computer systems. Systems belonging to the so-called artificial intelligence are emerging.

Systems of collecting, processing and archiving data concerning health condition and processes of diagnosis and treatment of patients are the basis for efficient functioning of the health care system at the individual, local, regional or central level. Currently, we can observe several significant phenomena in the field of health data processing:

1) Standardisation of trust services and technical solutions required for the creation of electronic documents and implementation in EU countries of the identification mechanisms necessary for their creation The problem of the current Polish health care system is the lack of tools for identification required for the service of health services (the so-called high level).
2) Changing the type of devices used for processing data from stationary to mobile. It should be noted that the mass transfer of operations performed so far by desktop computers and laptops to mobile devices - tablets, smartphones, etc. Should be noted. The use of devices supporting treatment processes as well as a wider and wider range of new diagnostics in relation to the patient results in the process of generating information that we have never had to deal with before.
3) Widespread use of cloud computing to process health data.
4) Generation and processing of health data, including their analysis by IT systems and technical devices without human intervention, the so-called artificial intelligence. Using big data algorithms to simulate future health care phenomena (e.g. maps of health needs).
5) Technologies that enable the personalisation of available data sets, previously considered as anonymous and not subject to regulations protecting personal data.
6) Attempting to introduce blockchain technology to securely collect patient data.

All these phenomena are related to the generation of more and more data and information about the patient's health. It is caused mainly by a greater number of recommended and technologically advanced diagnostics, but also by the introduction of analytical and settlement systems at the national and regional levels, as well as by a faster than so far process of introducing electronic databases. The classic division of data and information in health care depending on a (physical) data carrier is becoming a thing of the past. Classical medical documentation recorded on paper will still accompany the health care system, but the time is approaching when the final end of its creation will be reached. Paper-based documentation cannot meet the challenges of time. It is often more and more dispersed, and at the same time there is a lack of an entity that has the technical and legal capacity to coordinate all the patient's data. This increase in the amount of data and information processed requires authorised users to ensure proper, trouble-free processing and an adequate level of security. The article discusses the most important issues concerning the security of medical data in the light of new technological and legal challenges. Without their proper solution, both on the local and central level (health care information system), it is difficult to talk about building an efficient information system supporting the health care functioning.

II. PATIENT DATA SECURITY - DIFFERENT DATA SOURCES

It should be emphasized that only a small part of data and information about the patient's health is collected in the patient's medical records (the equivalent of which may today be an electronic patient record or a more commonly used name, an electronic health record). A large part of data and information is processed in numerous databases maintained by healthcare providers, payers, including the National Health Fund, entities obliged to keep medical records and by suppliers of devices and software, about the existence of which the patient often knows nothing. This does not mean, however, that information on health condition collected outside medical records is deprived of protection. Most data processors try to provide technical solutions that ensure their security. Some databases are protected by specific provisions.

Security of data and information collected about patients is to be ensured primarily by regulations dedicated to collecting and processing of data on health condition. They regulate in detail the processes of storage, transfer and protection of data obtained during the patient's stay in a medical entity, including, inter alia, determining the detailed scope of data on a specific patient, to which specific entities are entitled. However, all unregulated areas of health data processing are subject to the general provisions on the protection of personal data.

The development of technology and the emergence of the data market have caused considerable problems in the application of legal provisions in force in the EU.

Traditionally, regulations ensuring personal data protection divide protected data into two groups: data protection and data protection:

- ordinary data containing personal data not belonging to the group of sensitive (sensitive) data - this is the case, inter alia, in the labour code,
- a specific category of personal data (so-called sensitive data) - the catalogue of this category of data is defined and the breach may have more serious consequences than a breach of ordinary personal data.

In the literature on the subject, it is more and more often stated that the above section is outdated. The mechanism of ensuring the security of processed personal data, both ordinary and sensitive, is based on the belief that the entities that are legally empowered to process personal data will ensure their security. A category of data of particular importance for the privacy of an individual, the so-called sensitive data (e.g. health data, genetic data) was introduced and separate requirements for handling this group of data were created. This was intended to give confidence in the greater guarantees associated with the protection of special categories of data (sensitive data). Data processors must select appropriate techniques and organisation solutions to ensure that the data processed are properly secured. Whether the process of securing data adopted by the entity processing them is correct is subject to assessment by a specially appointed authority. Such a solution functioned for many years and was generally accepted. However, the development of data processing technology and post-universal turnover of personal data sets caused a situation in which most of the sets considered until recently to be impossible to identify nowadays become sets containing personal data.

At the same time, there is a concept of information autonomy, according to which individuals, by controlling the sharing of information about themselves, may effectively limit access to them, and consequently set a limit to the protection of their privacy. [1] The consequence of this state of affairs is the information obligation and the requirement of consent of the entity to process its personal data. The data subject should be informed about the processing of his or her data by a specific controller.

III. ENCRYPTION, PSEUDONYMISATION AND ANONYMISATION

RODO (General Data Protection Regulation 2016/679) indicates possible techniques that affect the security of the processed data. Their application results in the exclusion of the possibility of processing by unauthorized persons. The regulations indicate as recommended security techniques: data encryption and pseudonymisation. (Article 32) [2] At the same time, the rules provided for a situation in which very complex, time-consuming and costly steps were taken to identify individuals hidden by technical security measures. In such a case, however, the data thus concealed cannot be considered as personal data.

In both pseudonymisation and encryption techniques, it is possible to identify oneself using the appropriate keys under the control of the controller, and therefore personal data are still involved. This is not the case when an anonymisation technique is applied to public data. Anonymisation is not defined either in the Act on Personal Data Protection or in the RODO. Only recital 26 of the Preamble of the RODO mentions it. The definition is contained in ISO 9100:2011. This is a process by which information identifying a person is irreversibly altered in such a way that the

person (information subject) can no longer be identified, directly or indirectly, by the personal data controller or in cooperation with any other entity. Anonymisation is necessary, among others, to make available, for example, data on the state of health for scientific and research purposes.

IV. PROTECTION OF NON-PERSONAL DATA

From the end of 2018, non-personal data shall also be protected. Until now, mainly personal data to which identity can be attributed have been protected. The processing of other data was not regulated until the Regulation of the European Parliament and of the Council on the framework for the free movement of non-personal data in the European Union entered into force. [3] The main objectives of the Regulation are:

- to improve the cross-border mobility of non-personal data in the single market, which is currently hampered in many member states by location restrictions or legal uncertainty in the market,
- ensure that competent authorities retain full powers to request and access data for regulatory control, including inspections and audits,
- facilitate professional users to change service providers, store or otherwise process data and transfer their data without creating an undue burden on service providers or creating market distortions. [4]

This Regulation applies to non-personal data, i.e. data which in no way identifies a natural person. Non-personal data are all data that are not personal data within the meaning of the RODO (Article 3). [2] Such information includes, for example, information:

- information relating to the web pages viewed,
- data containing the number of visits and the time spent on a specific website,
- big data analyses,
- IT algorithms,
- data related to maintenance of industrial machinery,
- data produced by machines or anonymised data sets - unless this information relates to an identified or identifiable natural person.

Non-personal data are inextricably linked with personal data. In case of doubt, this Regulation will be superseded by the RODO. [5] There is also provision for data protection if technological developments make it possible to de-anonymise previously anonymised data, resulting in a change in their legal classification from non-personal data to personal data, in which case RODO will apply.

The principle of free movement within the European Union has been introduced for non-personal data, except where a restriction or prohibition would be justified for security reasons. In other words, it is not possible to indicate, for example, that data generated in health care must be processed only in a designated EU country where services have been provided.

It is also important to require that the relevant authorities have the power to request and access data for the purpose of regulatory control, inspections and audits. This will ensure that competent authorities cannot be denied access to data even though the data are processed in another Member State. An example is the control of electronic medical records processed in any EU country.

The protection of data on health condition classified for the most part as a specific category of data (so-called sensitive data) is to be ensured by appropriate legal regulations, both at national and EU level. The fundamental role is played by the RODO and the Act on Patients' Rights and the Act on Information Systems in Health Care. The recently adopted Polish law implementing the RODO has adapted nearly 170 different laws to the requirements of the EU data protection regulation. [6] This group includes regulations concerning medical professions and systemic regulations in the field of health care.

V. DATA PROTECTION OF INTERNET USERS

We are still working on a regulation supplementing the protection of e-Privacy personal data. [7] It is aimed at reducing the practice of uncontrolled processing of Internet users' data, which often results in significant interference with their privacy. It will specify, among others, the scope of technologies whose use will be subject to restrictions - cookies - but also any other technologies (e.g. so-called "pixels"; "web beacons"; "spyware"), which allow to identify or track the user, monitor his actions or locate. Simply mentioned is fingerprinting (i.e., tagging) technology, which enables the creation of a unique device identifier, without any information being placed on the user's device itself, by using a unique combination of information sent by the device while visiting websites or using applications. [8]

Most of the regulations currently being implemented and prepared are intended to contribute to ensuring data securi-

ty in the technology environment, which in general is largely incomprehensible to most people. Their main task is to implement and adapt the applied technological solutions to the ever-changing standards. This is primarily related to the fact that the data processing entity provides appropriate devices, software or access to solutions delivered via the network. It also requires the data processing entities to undertake a number of organisational and technical actions. Their result is to ensure cooperation, both in a specific unit and in the health care system, equipment and software, and to ensure the safety of operations.

The regulations indicate the use of the indicated techniques as those that will either contribute to the protection of personal data (encryption, pseudonymisation) or after the expiry of the purpose of processing (or the time limit for data storage required by law) will lead to a change in the category of personal data from personal data to non-personal data (anonymisation). They do not specify any specific recommended solutions. In this case, the legal basis for data protection is changed to a much less stringent one. Difficulties may be related to the assessment of the effectiveness of the technical solutions used to anonymise the data. A number of examples point to misapplication of these solutions.

VI. WHOSE OWNERSHIP IS IT OF THE PATIENT'S DATA?

The question arises as to who owns the data collected about the patient and who can process it outside of the patient. It seems that in the era of the information society this issue needs to be finally resolved. On the one hand, there is the right to privacy and the legally guaranteed access of patients to medical records. On the other hand, there is the public interest, which serves primarily to study phenomena occurring in health care, both for research purposes and to observe the demand for services and medicines, including simulating phenomena that will occur in a few years' time. It is worth noting that in the era of electronic medical documentation we do not solve the problem of ownership of the documentation itself, but the data contained in the documentation. Electronic medical documentation is each time created from data processed in electronic databases and serves for The postulated condition is full control of the patient over what data and information concerning him/her are stored, processed and made available. As a result, the patient has the right to require that the data concerning him/her obtained during the treatment process be used only to the extent that he or she accepts it. Only in exceptional situations, justified by the needs of the state, data may be processed by entities designated by law. The fundamental problem that arises is the real willingness of the patient to engage in the process of data control. However, it is not an easy solution to implement. There are two major barriers here:

- the patient's willingness to get involved in the process of controlling his or her health status,
- to make it technically possible for the patient to observe who is processing his or her health data.

In areas where there are legal regulations for the processing of health data, the patient usually receives information about the data collected about him or her. It is worse in situations where we are dealing with the Internet of Things (IoT) or autonomous devices belonging to the so-called artificial intelligence. The concept of IoT is widely used by the healthcare sector. Nowadays, almost every person has a mobile phone and usually it is a smartphone. This makes it possible to monitor the state of health, especially in older people. It is now possible to diagnose the patient's health condition at a distance and send the data to the doctor. Thanks to a system of sensors, e.g. at home, as well as personal belongings such as watches, jewellery or clothes, it is possible to monitor basic health parameters such as blood pressure, body temperature, glucose levels and heart rate. All data collected by the sensors can be transferred quickly to the doctor. In this way, they create electronic medical records of the patient. 9] Increasingly, applications are breaking down the history of our ailments, medications, and so on. Often, problems arise from determining the ownership of devices and software, which in turn raises the following questions: who is the owner of the collected data? Are there any restrictions on transferring data to third parties? [10] It can be assumed that in the coming years the "right to be forgotten" will be modified in order to extend this right also to the area of medical data.

A major challenge for legislation is to define the problem of ownership of patient data. This is related to the most important issue of the patient's role in the health care system. It is necessary to define concretely who is the owner of information about the patient, and not only those contained in medical records. The right of the patient to influence the scope of the data processed by him or her (consent to the processing of data and their scope) should be analyzed very carefully. As a result, the issue of who decides about collecting data in the patient's record, transferring them to other entities and deleting data from the record should be resolved. We are talking here about information

collected in one place and coming from different entities. This does not apply to documentation collected by entities providing health services in their databases and used for settlement purposes and possibly for evidentiary purposes in court cases.

VII. CONCLUSIONS

New regulations on the identification of trust services, personal data security and cyber-security will also have a broad application in health care. Most of them were issued in the form of regulations ensuring their universal applicability throughout the EU. Unfortunately, the implementation of new legal solutions at the level of health care may be difficult, if only because of the costs of implementation. Both the highly desirable system of identification of persons providing health services and patients, the universal implementation of trust services and the classification of some hospitals as operators of key services are very high financial burdens for medical entities. On this occasion, we may wonder whether at least some of the required solutions should not be financed by the state, e.g. issuing certificates for advanced electronic signatures and seals or making cloud solutions widely available for keeping electronic medical records:

- it is also worth noting the communication with the health care environment. Even if all the actions taken recently are right and generally acceptable to the environment, there is a lack of information about the projects being carried out and actions supporting the state in the process of computerisation. In other words, it is necessary to explain what are the objectives of long-term tasks undertaken, what tools are necessary for their implementation and what is the role and support of the state in the process of their implementation. First of all, it should be remembered that when defining the objectives, one should take into account both patients and the diverse environment of entities providing health services.

VIII. REFERENCES

[1] Rojszczak M. Definicja i granice prawnej ochrony prywatności w epoce analityki big data. RPiEiS 2019;81:115–28. http://dx.doi:10.14746/rpeis.2019.81.1.8

[2] Parlament Europejski. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[3] Parlament Europejski. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[4] Parlament Europejski. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej COM/2017/0495 final - 2017/0228 (COD).

[5] Gęsicka D. Dane nieosobowe - porządków w danych w Unii Europejskiej ciąg dalszy. [online] [cited 2019 August 24] Available from: URL: https://www.ipwsieci.pl/wpis,167,Dane_nieosobowe_-_porzadkow_w_danych_w_Unii_Europejskiej_ciag_dalszy.html .

[6] Sejm. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[7] Parlament Europejski. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej).

[8] Piechocki A, Siciński D. Cookies i podobne technologie w rozporządzeniu ePrivacy. GazetaPrawna.pl. [online] [cited 2019 August 24] Available from: URL: https:// serwisy. gazetaprawna.pl/nowe-technologie/ artykuly/ 1396917, rozporzadzenie-eprivacy-cookies-technologie.html.

[9] Smejda P. Internet rzeczy (IoT) we współczesnej gospodarce. Rola, zadania i bariery rozwoju. Zesz Nauk Org Zarz / Pol Łodz 2016;z. 64. [online] [cited 2019 September 24] Available from: URL:http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5e4510d7-dcf0-4aeb-a79c-5111c664f5a3.

[10] Maj I. Internet rzeczy i zagrożenia z nim związane. [online] [cited 2019 September 24] Available from: URL:.https://repozytorium.ka.edu.pl/handle/11315/20381.